ICT/MSP (2018) 601v1  
28/05/2018

**European Multi-Stakeholder**

**Platform on ICT Standardization**

**Title document:** **OAuth 2.0 authorization framework (IETF)**

**Final CAMSS Assessment report**

**For validation and advice by the MSP**

**Document for:**

|  |  |
| --- | --- |
| **Information** |  |
| **Decision** | **🗸** |
| **Discussion** |  |

**Email**:[ec-ict-std-platform@ec.europa.eu](mailto:ec-ict-std-platform@ec.europa.eu)

**CAMSS ASSESSEMENT REPORT**

**Technical Specification: OAuth 2.0 (IETF)**

This document is submitted to the MSP members by correspondence for consultation with a view to expressing advice in accordance with Articles **13 and 14 of Regulation EC 1025/2012** on the identification of OAuth 2.0.

The responsibility of advising the Commission on whether the technical specifications should be identified remains with the MSP.

**OAuth 2.0 has been positively evaluated by the CAMSS team** **following the MSP streamlined evaluation process (document ICT/MSP (2018) 014a rev 1).**

It is believed that as such OAuth 2.0 developed by IETF complies with the requirements for the identification of ICT technical specifications set by Annex II of Regulation (EU) No. 1025/2012.

In accordance with step 3 of the streamlined evaluation process, MSP members are invited to express their advice or any divergent views in written **by June 18th 2018**. The lack of opposition will be interpreted as an agreement with this assessment.

**The MSP advice would be considered to be positive and OAuth 2.0 will be considered eligible for identification by the Commission on the basis of CAMSS assessment report confirmed by the MSP so that once identified it shall constitute a “common technical specification” in the sense of Article 14 of the Regulation (EU) No. 1025/2012.**

# ASSESSMENT SUMMARY

**IETF OAuth 2.0 Technical specification**

**I. Introduction**

This document reports to the European Multi-Stakeholder Platform on ICT Standardisation, hereafter 'the MSP', on the assessment of a technical specification (TS), **OAuth 2.0** from **IETF.** This assessment has been performed by the CAMSS Team following the CAMSS MSP scenario assessment criteria which is in full compliance with Annex II criteria set out in the Regulation 1025/2012[[1]](#footnote-1), on European standardisation.

**II. Assessment Summary**

The OAuth 2.0 authorization framework is an open technical specification for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites without sharing their data.

During the assessment, evidence was found of the technical specification, OAuth 2.0, being satisfactorily compliant with the standardisation regulation Annex II criteria.

* **Market acceptance** of the technical specification is evidenced by the wide adoption of the TS by different suppliers and vendors.

OAuth 2.0 is used as a way for Internet users and developers to grant websites or applications access to their information on other HTTP applications without exposing their credentials.

This mechanism is used extensively by companies with an international market dominance such as Amazon,Google, Facebook, Microsoft and Twitter to allow the users to share information about their accounts with third party applications.

* **Coherence** of the TS is evidenced by the fact that there is no existing European standard or technical specifications being under consideration to become a European standard that has the same area of application as OAuth 2.0.
* **IETF is a non-profit organisation which follows an open process.** TheMSP has already identified TS of IETF in the past, and positively evaluated the compliance of its process with Annex II criteria.
  + 1. **Openness of** the TS is evidenced by the openness of IETF to newcomers. There is no formal membership.
    2. **Consensus** and continuous consent of the community is required during the several iterations carried out during the development of the TS, as all IETF technical specifications.
    3. **Transparency** is evidenced by the availability of the documentation during the development period of the TS**.** The IETF Datatracker is the day-to-day front-end to the IETF database for people working on IETF standards. It contains data about the documents, working groups, meetings, agendas, presentations and more, of the IETF.
* **The TS meets adequate requirements** set out in Annex II §4
  + 1. **Maintenance**

OAuth is an IETF standard, and as such it follows the defined and publicly available set of processes for the modification and revocation of standards defined in sections 6.3 and 6.4 of its Internet Standards Process[[2]](#footnote-2).

* + 1. **Availability**

As all the IETF standards, OAuth 2.0 is a free and open TS, and it is available for use at the corresponding IETF repository[[3]](#footnote-3).

* + 1. **Intellectual Property Rights (IPR)**

OAuth 2.0 is licensed by the IETF Trust. It is subject to BCP 78[[4]](#footnote-4) and the Trust Legal Provisions in force on the date of TS publication[[5]](#footnote-5). IPR claims relating to the TS are available from the IETF Datatracker IPR Search tool[[6]](#footnote-6). It is therefore licensed on a royalty-free basis.

* + 1. **Relevance**

OAuth 2.0 contributes to interoperability between public administrations by enabling the delegation of access to protected resources for client applications between them, which is evidenced by several existing implementations and references. Therefore it addresses public policy objectives, and example of which would be the NIS Directive[[7]](#footnote-7). Regarding societal needs, it tackles the increasing need for security in some of the most breaking-edge technologies at the moment, like it is the case of IoT[[8]](#footnote-8).

* + 1. **Neutrality and stability**

OAuth 2.0 keeps no dependencies on other specific products, platforms or technologies; and has reached maturity and stability.

* + 1. **Quality**

OAuth 2.0 has sufficient detail, consistency and completeness for the use and development of products and services. It is evidenced by its wide use as a security TS for phones, tablets, wearables, and internet of things devices.

**III. Assessment Results**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Category** | **Automated Score** | **CAMSS Strength** | **# Favourable** | **# Unfavourable** | **# Not Applicable** |
| Market acceptance | 100 % | 100 % | 3 | 0 | 0 |
| Coherence principle | 100 % | 100 % | 3 | 0 | 0 |
| Attributes | 100 % | 100 % | 6 | 0 | 0 |
| Requirements | 100 % | 100 % | 9 | 0 | 0 |
| **Overall Score:** | **100%** | **100 %** | **21** | **0** | **0** |

This section presents an overview of the results of the CAMSS assessments for OAuth 2.0. The CAMSS “Strength” indicator measures the reliability of the assessment by calculating the number of answered (applicable) criteria. On the other hand, the number of favourable answers and the number of unfavourable ones are used to calculate the “Automated Score” per category and an “Overall Score”.

The results of the CAMSS assessment, with a 100% CAMSS Strength, can be considered as truly representative of the specification attributes. Furthermore, a 100% Automated Score demonstrates that the technical specification is fully compliant with the CAMSS MSP scenario assessment criteria and therefore with standardisation regulation Annex II. The Overall Score is 100%, so it reflects that OAuth 2.0 fully meets the criteria regarding Market Acceptance, Coherence, Attributes and Requirements.

**IV. Assessment Observations**

During our assessment, the observation has been made that OAuth 2.0 has been particularly criticized due to the huge difference with its first version. OAuth 2.0 is less secure and more complex than its predecessor OAuth 1.0. This is because version 2.0 creators deliberately focused on making the technical specification more flexible between sites and devices. The changes are so significant that OAuth 2.0 is not backward compatible.

Due to the aforementioned intention to make OAuth 2.0 a rich and highly extensible framework with many optional components, an OAuth 2.0 implementation might be non-interoperable with another. Additional agreements like application profiles prevent different implementations and thus improve interoperability. Also, OAuth 2.0 does not support encryption, signature or client verification directly. Instead, OAuth 2.0 expects implementers to use an outside protection protocol, which caused security vulnerabilities.

However, the aforementioned issues did not prevent OAuth 2.0 to impose itself since several years as a standard security framework for transmitting authorization decisions across a network of web applications and APIs. The version 2.0 of the technical specification is today widely adopted, notably by internet giants as Facebook or Google.

# CAMSS PRE-EVALUATION RESULTS

**Introduction[[9]](#footnote-9)**

This section provides the European Multi-stakeholder Platform on ICT Standardisation with preliminary findings to help it on the evaluation of the specification "OAuth 2.0” for identification pursuant to article 13 and Annex II of Regulation (EU) No. 1025 /2012[[10]](#footnote-10).

The report covers the following detailed assessments on Annex II criteria of the European standardisation regulation:

1) Compliance with the "market acceptance" and "coherence" criteria set out by Annex II. §1 & §2; providing information on the proposed ICT technical specifications in relation to the formal European standardisation system and related standardisation activities.

2) Characteristics of the organisation and its technical specification developing procedures in accordance to Annex II.3.

3) Compliance with the requirements for the identification of ICT technical specifications set out by Annex II.4.

# 1. Pre-report to the platform

**1.1 Subject of the evaluation[[11]](#footnote-11)**

OAuth 2.0 is the latest version of the OAuth protocol which was originally developed by Google in late 2006. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. This specification has been developed within the IETF OAuth Working Group, is not backward compatible with its previous versions and is considered a framework for authorization delegation between third parties.

OAuth 2.0 provides clients with a "secure delegated access" to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. Designed specifically to work with Hypertext Transfer Protocol (HTTP), OAuth essentially allows access tokens[[12]](#footnote-12) to be issued to third-party clients by an authorization server, with the approval of the resource owner. The third party then uses the access token to access the protected resources hosted by the resource server.

OAuth 2.0 is commonly used by Internet users to grant websites or applications access to their information on other website without sharing any credentials. This mechanism is used by companies such as Amazon, Google, Facebook, Microsoft and Twitter to allow the users to share information about their accounts with third party applications or websites.

**1.2 Possible links with other ICT technical specifications or standards**

The integration of applications and services external to the organisation’s domain is nowadays a common approach. This implies the management of the authentication and authorization for the entities aiming to consume the Application Programming Interfaces (APIs). The aforementioned implementation requires service-oriented architectures associated with a single sign-on (SSO) strategy. In this context, federated identities are used in order to link electronic identities a user has across identity management systems.

Federated identities’ benefits are related to the management of authentication and authorisation but also to enhance the end-users’ experience. The protocols with a significant market share of adoption employed for federated identity implementations are OpenID Connect, SAML v2.0, and OAuth 2.0.

SAML 2.0 (Security Assertion Mark-up Language) is the oldest of the three technical specifications and deals with both authorization and authentication. The technical specification is widely applicable but its common usage is especially focused on enterprise SSO unlike OAuth 2.0, which does not cover authentication and is designed for use with web applications on the Internet.

OpenID was originally an open standard for authentication that is completely different from OAuth. However, its latest version, called OpenID Connect, combines OpenID authentication and OAuth 2.0 authorization.

Since OpenID Connect covers both authentication and authorisation and that encompasses OAuth, it is more comparable to SAML 2.0 than to OAuth 2.0. OpenID Connect is considered as the future of authentication and authorization particularly because it was developed with the perspective of being implemented within mobile and native apps.

# 2. Evaluation of compliance

**2.1 Market acceptance**

OAuth 2.0 has large market acceptance and there is no known issue regarding its interoperability.

Market acceptanceis evidenced by several implementations of the TS proving the existence of a wide customer base between both open source and commercial implementations. This is a consequence of apps becoming the new intermediaries of the markets and needing a way to create trust, which at the same time is a consequence of the actual market trend being the expansion of open platforms. Open platforms allow developers to decouple partners from the platform’s business cycle making their growth faster, and therefore reaching a critical mass that leads them to market dominance in less time. This tendency is called low-friction innovation. In this context, in which apps are developed in a short time period and often with rather short lives, the traditional way of creating trust through a continued use has turned obsolete.

In order to cover this gap, new specifications like OAuth 2.0 have arisen as an alternative way of creating trust through the provision of access to information in the apps without the need for exposing the user credentials.

Between the various implementations of the TS that back this reasoning, the most remarkable ones are the following:

* Linkedin[[13]](#footnote-13)
* Facebook[[14]](#footnote-14)
* Apple[[15]](#footnote-15)
* Google[[16]](#footnote-16)
* Amazon[[17]](#footnote-17)
* Microsoft[[18]](#footnote-18)

Interoperability in those implementations is largely accountable on the fact that OAuth 2.0 is interoperable with most technologies. That said, due to OAuth 2.0 being highly extensible and therefore accepting many optional components, it could be the case that an OAuth 2.0 implementation was not interoperable with another OAuth 2.0 implementation.

In order to prevent this and foster interoperability, additional agreements like application profiles can be reached.

**2.2 Coherence with the formal European standardisation environment**

*2.2.1 The specification covers a domain where the adoption of a new European standard or standardisation deliverable is not foreseen within a reasonable period.*

OAUTH 2.0 covers an area, which is the provision of specific authorization flows for web applications, desktop applications, mobile phones, and living room devices; that is actually not covered by any other technical specification being under consideration to become a European standard. This conclusion has been withdrawn from the examination of all the programming mandates addressed to CEN, CENELEC and ETSI to the date, CEN’s webpage[[19]](#footnote-19), CENELEC’s webpage[[20]](#footnote-20), CEN-CENELEC’s webpage ICT section[[21]](#footnote-21), the EC Information Providers Guide, Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies[[22]](#footnote-22), the standards and tools for exchange and processing of actionable information inventory of ENISA[[23]](#footnote-23) and the ENISA Programming Document 2018-2020[[24]](#footnote-24).

*2.2.2 The current scope of the formal European standardisation organisations does not cover any similar domain*

No overlap has been detected with European standardisation organisations activities at EU level.

This conclusion is based on the work programmes of CEN and CENELEC[[25]](#footnote-25), and ETSI[[26]](#footnote-26) as published on their respective websites, and on the ENISA Programming Document 2018-2020[[27]](#footnote-27).

*2.2.3 Transposition of the proposed ICT technical specification into a European standard or standardisation deliverable is not foreseen within a reasonable period.*

Having checked the documentation included in point 2.1.1 we have gotten to the conclusion of that OAuth 2.0 is not foreseen to be transposed into a European standard within a reasonable time period.

*2.2.4 For information, related initiatives*

No other related initiatives have been found.

# 3. Evaluation of compliance with the attributes

**3.1 The organisation developing the specification[[28]](#footnote-28)**

IETF is an unincorporated, freestanding organization constituted by an open and international community of members from a wide variety of backgrounds. Its aim is the development of standards to help the correct functioning of the Internet.

**3.2** The development process

Despite OAUTH being originally developed by Google, OAuth 2.0 is a specification maintained by the IETF, and the IETF has a defined process for the development of standards[[29]](#footnote-29). This process is based on a development stage followed by a set of iterations carried out on the basis of the reviews made by the SDOs’ community.

1. **Openness**

The IETF development process is open for participation, what can be deducted from the fact that it provides a large number of opportunities for participation to all interested parties. At each stage of the development process the specification is exposed to open discussion and its characteristics are debated in open meetings and/or public electronic mailing lists. In addition, the specifications are made available for review via world-wide online directories. These facts are detailed in section 1.2 of the IETF development process[[30]](#footnote-30).

In addition, the IETF publishes the information collected by the different working groups that develop the specifications in the shape of Requests for Comments (RFCs) in a repository[[31]](#footnote-31).

1. **Consensus**

The IETF sets a series of conditions for the adoption of a specification as Internet Standard through its development process. These conditions explicitly state that for a specification to be recognised it has to answer to generally-accepted practices. This means that the candidate specification must be implemented and tested to check its correct operation and interoperability by multiple independent users; and used in increasingly-demanding environments. These facts are detailed in section 1.2 of the IETF development process[[32]](#footnote-32).

1. **Transparency**

All the IETF specifications are available free of charge via their website[[33]](#footnote-33). In addition, the IETF Datatracker[[34]](#footnote-34) is a public database in which the work for the development of the specifications is documented and accessible by any interested party. It contains documentation regarding multiple aspects of the work carried out by the IETF, like working groups, meeting minutes or presentations.

Finally, the IETF also maintains an Internet Draft’s Directory[[35]](#footnote-35) in which all the information regarding the on-going specifications’ development process is made available publically.

These factors show a high degree of transparency in the specifications’ development process.

**3.3 The specification**

**3.3.1.** Maintenance

The IETF has a defined maintenance process for its standards. It is included in section 6.3 of its Internet Standards Process[[36]](#footnote-36) a defined method for the revision of its standards. According to it, when a new version of a standard is released it shall undergo the full Internet Standards Process to be endorsed by the IETF as one of its standards. Normally this process ends with the substitution of the old version of the standard for the new one, but in some cases both versions will remain coexisting. In this case the relationship between both shall be clearly defined rather in the text of the new version of the specification or in a document designed to that end.

**3.3.2. Availability**

OAuth 2.0 is publicly available for download, implementation and use on reasonable terms in IETF’s webpage[[37]](#footnote-37).

**3.3.3. Intellectual Property Rights rules**

IETF has a defined and publicly available policy about Intellectual Property Rights (IPR), such as patent rights, relative to technologies developed in the IETF. Like all the IETF standards, OAuth is a free and open technical specification, built on IETF standards and licenses. It is subject to BCP 78 and the Trust’s Legal Provisions in force on the date of TS publication. IPR claims relating to the TS are available from the IETF Datatracker IPR Search tool. OAuth is therefore licensed on a royalty-free basis.

**3.3.4. Relevance**

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service; or by allowing the third-party application to obtain access on its own behalf.

OAuth contributes to the interoperability between public administrations by enabling the delegation of access to protected resources for client applications between them, what is evidenced by several references and implementations. Between these implementations, WeGovNow aims at creating an implementation that is fully compliant with the OAuth 2.0 Authorization Framework: the “Unified WeGovNow User Management” module. In addition and as previously mentioned in section 2.1 of this report, OAuth 2.0 has been implemented by a large set of companies with an absolute dominance in their markets.

OAuth 2.0 clearly provides security and reduces privacy risks. The added value of this technical specification is that providers of online services will not acquire log-in data from users in order to allow them to use other online services. The result is reduction of privacy and identity-theft risks, and misuse of identity data. It also allows web and mobile applications to integrate securely with each other. For example, within mobile services using RESTful APIs OAuth 2.0 can be used to take care of the authorization.

Therefore, through its purpose to give users more control over their data, OAuth addresses societal needs and public policy objectives.

**3.3.5. Neutrality and stability**

The Internet Engineering Task Force (IETF) is the premier Internet standards body, developing open standards through open processes. As an IETF standard OAUTH 2.0 has been developed through the use of an open and consensus-based process. It is an open standard, and it has been implemented by a large set of different stakeholders with a clear dominance in their respective markets (See section 2.1). There is no known interoperability issues between it and any other standards, and it has been in use for a sufficient time to be considered as a stable standard.

Therefore, it shall be considered a neutral and stable standard.

**3.3.6. Quality**

The sufficient detail, consistency and completeness for the use and development of products and services of OAuth2.0 is incontestable. It is evidenced by the wide use of OAuth 2.0 as a security standard for phones, tablets, wearables, and internet of things devices. A familiar example for users is the possibility to log in to a particular online service using a Google, Github or Facebook account.

However, OAuth 2.0 has been proved to have Covert Redirect Vulnerabilities. A Covert Redirect is an app that takes a parameter and redirects a user to the parameter value without sufficient validation. This particular vulnerability is not a direct consequence of the use of OAuth 2.0 itself, but of an excess of confidence on the clients. In this sense, OAuth 2.0 expects to receive lists of trustworthy domains and assumes their safety, while this is not always the case.

However, as it is not a particular security breach derived from the use of the specification it cannot be stated that OAuth 2.0’s quality can be undermined by it. Also, security considerations[[38]](#footnote-38) were defined base on a threat model for the OAuth protocol in order to complement those included in the OAuth specification.

1. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1025&from=EN> [↑](#footnote-ref-1)
2. <https://www.rfc-editor.org/rfc/rfc2026.txt> [↑](#footnote-ref-2)
3. <https://tools.ietf.org/html/rfc6749> [↑](#footnote-ref-3)
4. <https://www.rfc-editor.org/rfc/rfc5378.txt> [↑](#footnote-ref-4)
5. <http://trustee.ietf.org/license-info/IETF-TLP-4.pdf> [↑](#footnote-ref-5)
6. <https://datatracker.ietf.org/ipr/search/?rfc=6749&submit=rfc> [↑](#footnote-ref-6)
7. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN> [↑](#footnote-ref-7)
8. <https://nordicapis.com/why-oauth-2-0-is-vital-to-iot-security/> [↑](#footnote-ref-8)
9. We keep the section names of the official MSP Evaluation Report in order to ease the re-use of information [↑](#footnote-ref-9)
10. Regulation (EU) No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European Standardisation. OJ L 316/12 of 14.11.2012 [↑](#footnote-ref-10)
11. [https://www.w3.org/TR/OAUTH 2.011/](https://www.w3.org/TR/xhtml11/) [↑](#footnote-ref-11)
12. <https://tools.ietf.org/html/rfc6750#section-1> [↑](#footnote-ref-12)
13. [https://developer.linkedin.com/docs/OAuth2](https://developer.linkedin.com/docs/oauth2) [↑](#footnote-ref-13)
14. <https://developers.facebook.com/docs/facebook-login/manually-build-a-login-flow> [↑](#footnote-ref-14)
15. <https://developer.apple.com/documentation/accounts/acaccountcredential/1507896-init> [↑](#footnote-ref-15)
16. <https://developers.google.com/identity/protocols/OAuth2> [↑](#footnote-ref-16)
17. <https://aws.amazon.com/es/blogs/compute/introducing-custom-authorizers-in-amazon-api-gateway/> [↑](#footnote-ref-17)
18. [https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-protocols-OAuth-code](https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-protocols-oauth-code) [↑](#footnote-ref-18)
19. <https://standards.cen.eu/> [↑](#footnote-ref-19)
20. <https://www.cenelec.eu/> [↑](#footnote-ref-20)
21. <https://www.cencenelec.eu/standards/Sectors/ICT/Pages/default.aspx> [↑](#footnote-ref-21)
22. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2102&qid=1521731286208&from=ES> [↑](#footnote-ref-22)
23. <https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport> [↑](#footnote-ref-23)
24. <https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020> [↑](#footnote-ref-24)
25. <https://www.cencenelec.eu/News/Publications/Publications/WorkProgramme-2018_UK_acces.pdf> [↑](#footnote-ref-25)
26. <http://www.etsi.org/images/files/WorkProgramme/etsi-work-programme-2017-2018.pdf> [↑](#footnote-ref-26)
27. <https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020> [↑](#footnote-ref-27)
28. <https://www.ietf.org/> [↑](#footnote-ref-28)
29. <https://www.ietf.org/standards/process/> [↑](#footnote-ref-29)
30. <https://www.rfc-editor.org/rfc/rfc2026.txt> [↑](#footnote-ref-30)
31. <https://www.ietf.org/standards/rfcs/> [↑](#footnote-ref-31)
32. <https://www.rfc-editor.org/rfc/rfc2026.txt> [↑](#footnote-ref-32)
33. <https://www.ietf.org/standards/> [↑](#footnote-ref-33)
34. <https://datatracker.ietf.org/> [↑](#footnote-ref-34)
35. <https://www.ietf.org/standards/ids/> [↑](#footnote-ref-35)
36. <https://www.rfc-editor.org/rfc/rfc2026.txt> [↑](#footnote-ref-36)
37. https://tools.ietf.org/html/rfc6749 [↑](#footnote-ref-37)
38. <https://tools.ietf.org/html/rfc6819> [↑](#footnote-ref-38)